STATEMENT OF
JACQUELYN L. WILLIAMS-BRIDGERS
INSPECTOR GENERAL OF THE
U.S. DEPARTMENT OF STATE,
ARMS CONTROL AND DISARMAMENT AGENCY, AND THE
UNITED STATES INFORMATION AGENCY, INCLUDING
INTERNATIONAL BROADCASTING

FOR THE

COMMITTEE ON FOREIGN RELATIONS
SUBCOMMITTEE ON INTERNATIONAL OPERATIONS
UNITED STATES SENATE

MARCH 4, 1999

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to testify before your subcommittee on the major management challenges facing the Department of State. As my office also oversees the United States Information Agency (USIA), including international broadcasting, and the Arms Control and Disarmament Agency (ACDA), my testimony will incorporate some management challenges that apply to all three agencies.

Summary

My office has identified several significant challenges facing the agencies that we oversee. Foremost among these is the safety and protection of our people, facilities, and information. The scope and gravity of this challenge was brought into clear focus by the attacks on U.S. embassies in Africa last year. The Department is faced with the immediate need to address physical security vulnerabilities and enhance emergency planning at our overseas posts. Longer-term challenges include major embassy renovations to improve security, new embassy construction, and the maintenance of security equipment. To meet these challenges, the Under Secretary for Management has created a number of coordinating groups to which she has welcomed full OIG participation.

Another critical challenge facing the foreign affairs agencies is their vulnerability to the Year 2000 (Y2K) problem. Generally, the Department is making steady progress toward preparing computer systems for the Year 2000 date change, and estimates that 55 of 59 mission-critical systems will be implemented by the Office of Management and Budget's (OMB's) deadline of March 31, 1999. Successfully meeting the Y2K challenge is necessary to avoid havoc in the foreign affairs community, including disruption of messaging systems, impediments to embassy operations such as visa and passport processing, and failures in administrative functions such as payroll and personnel processing in the Year 2000.

Despite this progress, we are concerned that the Department's Y2K certification process, which is designed to provide documented independent assurance that all possible steps have been taken to prevent Y2K-related failures, is proceeding too slowly. Thus far, only two mission-critical systems have been certified by the Department's Y2K Certification Panel. According to the General Accounting Office's Year 2000 Assessment Guide, agencies should consider subjecting their Year 2000 program to certification, which, in essence, is an independent verification and validation that all necessary steps to achieve Y2K compliance have been taken. Further, verification and validation may be performed by the agency's quality assurance staff complemented by internal auditors.

Other major challenges faced by the Department include the need to strengthen border security, link resources to policy priorities, consolidate the foreign affairs agencies, correct weaknesses in financial management, and improve real property management and maintenance. Before I provide additional details on these challenges, I would like to give you a sense of OIG's mission and responsibilities, as well as provide a brief overview of our strategic plan.

OIG Operations

OIG Organizational Structure

The mandate of my office is to improve the economy, effectiveness, and efficiency of the Department of State (the Department), ACDA, USIA, and the Broadcasting Board of Governors and to detect and prevent waste, fraud, and mismanagement. Toward this end, OIG is composed of four operational offices that carry out inspections, audits, and investigations.

Office of Audits. OIG's Office of Audits consists of seven divisions, each with a specific area of focus: Consular and International Programs, Information Management, Financial Management, Property Management and Procurement, International Broadcasting, Human Resources, and Contracts and Grants. Audits conducted by these divisions assess management and financial operations and the economy or efficiency with which an entity is managed. Examples of reviews the Office of Audits is currently conducting include the Department's Consular Fraud Program, Year 2000 (Y2K) remediation efforts, implementation of the International Cooperative Administrative Support Services (ICASS) system, management of overseas property, and financial statement preparation.

Office of Inspections. OIG is required by law to routinely inspect the activities of overseas posts and domestic bureaus. These inspections are conducted to provide overseas missions and domestic bureaus information about the effectiveness of their performance and the quality of their management and operations through an assessment of three primary areas: policy implementation, resource management, and management controls. In FY 1998, the office inspected posts in 32 locations, including Russia, China, Thailand, and several African countries.

Office of Security and Intelligence Oversight. Through audits and inspections, the Office of Security and Intelligence Oversight evaluates the ability of overseas posts to respond to threats from terrorism, mobs, or other physical intrusion, intelligence penetrations, and crime. The office also evaluates whether the Department's security and intelligence programs and activities are being carried out with the most effective use of resources and in accordance with the law. Our security oversight inspection program supports the Secretary of State's statutory responsibility for the security of all nonmilitary U.S. personnel, property, and information abroad. In the aftermath of the Africa bombings, the OIG received strong Congressional support to significantly expand our security oversight work.

In an effort to add greater rigor to OIG's intelligence oversight responsibilities, I created an Intelligence Oversight Division within the Office of Security and Intelligence Oversight. The division reviews foreign policy aspects of programs and functions involving components of the intelligence community and identifies key areas of concern in the review of intelligence oversight and coordination by chiefs of mission.

Office of Investigations. The Office of Investigations performs investigations of criminal, civil, and administrative misconduct related to organizational programs and operations. Additionally, the office manages a Hotline for employees who wish to disclose potential fraud, waste, and mismanagement. The office also focuses on fraud prevention by increasing employee awareness and understanding of the standards of conduct and accountability and by reducing areas of vulnerability and opportunities for misconduct. We publish "Standards of Conduct," a guide to ethical conduct, which is issued to each employee in the Department, USIA, and ACDA. My office also issues fraud alert bulletins and management implication reports when our work identifies systemic weaknesses that have agency-wide or bureau-wide implications.

Followup and Resolution

Once an OIG report is issued, Department bureaus or posts with responsibility for implementing the report's recommendations have 45 days in which to respond. The responses are reviewed by OIG to determine whether they meet the intent of the recommendation. In the event that the bureau or post does not accept the recommendation as written, OIG can either accept the suggested alternative, if any, or refer the decision to the next management level for reconsideration. If an impasse is reached in resolving a recommendation, it is referred for decision to the Under Secretary for Management or, ultimately, to the Secretary of State or agency director.

The OIG semiannual report to the Congress identifies significant audit recommendations without management decision for more than six months, and significant recommendations reported previously, but still pending final action. In addition, the Secretary or agency Director is currently required to report to the Congress annually on any significant recommendations that have been agreed to but not

implemented for over one year. Our most recent semiannual report shows outstanding OIG recommendations in areas identified as management challenges, including maintenance and repair of buildings overseas, financial system acquisition and development, mainframe systems security, and management of secure communications.

OIG Strategic Plan

The Secretary of State has established seven broad national interests which provide the strategic framework within which the OIG conducts its integrated program of audits, inspections, and interdisciplinary reviews to evaluate progress toward achieving the Secretary's objectives. OIG's strategic plan establishes the OIG-wide goals that guide the work we will undertake into the 21st century. OIG strives to be proactive in addressing foreign affairs agencies' efforts to effectively implement U.S. foreign policy; clearly link resources to policy objectives; and maintain efficient, effective, and secure operations and infrastructures. We are committed to protecting the Secretary of State's ability to pursue the foreign policy objectives of the United States free from the impediments of waste, fraud, and mismanagement.

I would like to turn now to a more detailed discussion of the major management challenges facing the Department in the context of OIG strategic objectives.

Improved Implementation of Foreign Policy

The successful development and implementation of U.S. foreign policy depends on many factors. These include a clear understanding of foreign policy goals, coordination among the various agencies and entities with foreign policy interests, and clear and consistent lines of communication between the President, the Secretary of State, and the internal components of the Department.

Strengthening Border Security

Over the past few years, the Department has maintained a strong emphasis on the need to improve border security, however, the passport process and the immigrant and nonimmigrant visa processes remain material weaknesses. Improvements needed to address these weaknesses include additional management positions to support consular automated systems, and expanded intelligence information sharing among U.S. Government agencies. In terms of consular staffing, our own work has shown that the Department will face severe shortages of experienced midlevel managers for the next several years. We have also pointed out the need for more senior, experienced consular officers at posts with high fraud levels.

The Department has mounted a major effort to counter visa fraud, including initiatives such as the machine-readable visa program, worldwide advisories to overseas posts on detecting fraudulent documents, and programs to detect terrorists. The Department also continues to refine its consular lookout systems to identify names with different spellings or those that may be translated into multiple spellings. This will better enable the Department to identify individuals who should not receive visas. The

Department has also implemented a photo-digitized passport process which improves the ability to associate the document with the holder. OIG is currently reviewing the Department's consular fraud prevention efforts, including the adequacy of the Department's guidance and training in fraud prevention and the coordination of antifraud efforts.

Our work has facilitated several improvements in the Department's consular operations. For example, our recommendations helped ensure that the modernized version of the machine-readable visa system has the capability to electronically transmit relevant data on visa issuances to the Interagency Border Inspection Service for transmission to ports of entry. Also, our work encouraged the Department to establish a proactive program to identify individuals ineligible for a nonimmigrant visa in its computer system, such as drug traffickers, alien smugglers, and organized crime members. Additionally, an OIG recommendation contributed to the Department's ensuring that consular officers overseas have access to information on individuals from high-risk countries listed on the Department's CD ROM.

OIG also recently issued an inspection report on the U.S. border crossing card (BCC) replacement program for eligible citizens of Mexico. The program is a partnership between the Department and the Immigration and Naturalization Service. The "laser visa" replaces the BCC and is more tamperproof than previous documents; however, many problems reduce the effectiveness of the program. The lack of laser visa processing equipment at consular posts in Mexico and continued issuance of nonbiometric 10-year visas are problems that must be addressed by the Department. The Immigration and Naturalization Service, which has experienced delays in card production, checks applications against an inadequate criminal database, and has no plans to check each alien's identification card at the border. Efforts by both the Department and the Immigration and Naturalization Service will be needed to correct these problems. The issues jeopardize the timely implementation of the program and compromise its enhanced border security protection.

Better Alignment of Fiscal and Human Resources with U.S. Foreign Policy Priorities

The Government Performance and Results Act (Results Act) requires Federal agencies to set goals for program performance and to measure results with the goal to improve the efficiency and effectiveness of Federal programs. Specifically, the law requires that each agency submit to Congress and OMB a 5-year strategic plan for program activities. The plan is to contain goals and objectives, and describe how they will be achieved. Each agency is also required to submit an annual performance plan with measurable goals and indicators that link to the strategic plan.

Over the past three years, strategic planning efforts as required by the Results Act have prompted notable improvements in the Departments planning process. For example, at posts overseas there is increased focus and discussion on the U.S. Government's

overall goals in each country. Also, there is an improved collective assessment of all U.S. Government resources available at each post to achieve specific mission goals.

The challenge that exists for the Department and its partners in the foreign affairs community is to define goals stated in mission, bureau, and Department plans in more measurable terms, and in terms of outcomes--what the U.S. hopes to achieve--rather than broad policy statements. In addition, the Department needs to establish a credible system that will allocate resources across geographic boundaries.

The upcoming merger of foreign affairs agencies will provide an opportunity to realign foreign affairs resources with policy priorities. Effective integration of the foreign affairs agencies will depend, in large part, on the success of merging diverse personnel systems, adapting varied and diverse information systems, and melding complex financial systems.

Strategic Planning

The Department has revised its longstanding planning process to comply with the Results Act and developed a strategic plan containing 16 international affairs strategic goals and 3 diplomatic readiness goals. The Department then asked each post and bureau to submit a plan and budget linked with the Department's strategic goals. At the request of the Department, OIG has been active in reviewing the mission and bureau planning process.

Mission Performance Plans are the principal vehicle for documenting and reaching interagency consensus on country-level goals and strategies. The Mission Performance Plans, in turn, serve as building blocks for the Bureau Performance Plans, and ultimately, the Department's budget submission to OMB. However, OIG found, among other things, that the process used during FY 1998 to develop Mission Performance Plans was poorly timed and that many plans were incomplete. In addition, in the absence of an agreed upon set of performance measures, missions presented performance indicators that were inconsistent and sometimes irrelevant or difficult to track. Further, the software intended to link budgets with goals and objectives, the Resource Allocation and Budget Integration Tool proved cumbersome, ineffective and difficult to deploy. These problems resulted in corresponding weaknesses in the Bureau Performance Plans.

To date, the Department has been unsuccessful in implementing Results Act requirements for performance plans. The Department's FY 1999 Performance Plan, which was developed from the Bureau Performance Plans, did not comply with the Results Act, and both Congress and the Department identified several deficiencies with the plan. For example, the plan lacked baselines and performance targets, omitted management initiatives, contained goals that were broadly stated and extended beyond the Department's span of control, and provided little information on the resources required to achieve specific performance goals.

Although the combined FY 1999-2000 performance plan still does not fully comply with the Results Act, it is an improvement over the previous plan. For instance, the Department decided to focus its initial attention on the management bureaus, and as a result, the plan contains a comprehensive set of performance goals, baselines, and targets for the Department's diplomatic readiness goals. However, the sections in the plan on the 16 strategic goals are incomplete, providing only one example under each strategic goal. For example, under the strategic goal on regional security, the Department provides a performance goal, indicators, baselines, and targets only for its efforts in Northern Ireland. The Department states that it discussed its proposed FY 1999-2000 plan with Congress, GAO and OMB last Fall, and intends to work together with them to develop a performance plan that encompasses all of the Department's activities.

OIG will continue to assess the Department's progress in implementing the Results Act, and will take steps to verify and validate selected performance data. In addition, our audits will include reviews of the performance measures related to the areas reviewed. For example, our review of foreign trade barriers will determine whether the Department's FY 1999 performance goals, indicators, and information sources accurately reflect its progress in opening foreign markets in the telecommunications industry.

Distributing Costs of the U.S. Government Presence Overseas

The International Cooperative Administrative Support Services (ICASS) system was initiated in 1996 in response to a congressional mandate to implement a system that allocates to each department and agency the full cost of its presence abroad. Additionally, ICASS was intended to provide posts more control of administrative services through local empowerment, equity in cost distribution, transparency in billing, local selection of service providers, and the establishment of customer service standards. The goal was to obtain quality services at the lowest cost. OIG initiated a review of the ICASS program to assess posts' progress in selecting the most cost-effective service providers.

Our work to date has generally shown that most agencies at post consider ICASS an improvement over past cost distribution systems. ICASS councils, however, have not yet sought out more cost-effective service providers. There are a number of reasons for this, including the process for selecting alternate providers is unclear, post ICASS councils lack training and expertise in selecting alternate service providers, and ICASS councils cannot compel agencies to participate in what may be a more cost-effective solution for the U.S. Government through economies of scale.

One of the basic premises of ICASS is agency freedom of choice. At some posts, a few agencies have opted out of ICASS services. While those agencies have reported reducing their operating costs from what ICASS charges, the total U.S. Government costs may be higher since costs were redistributed among the agencies that did not opt out and ICASS staffing levels remained the same. We also found that some posts have not fully implemented ICASS, and ICASS information is not being used within Department headquarters elements to seek out more cost-effective alternatives.

Consolidating Foreign Affairs Agencies

The Omnibus Consolidated Appropriations and Emergency Supplemental Appropriations Act for FY 1999 mandated the consolidation of the Department of State, the Arms Control and Disarmament Agency, and the United States Information Agency into one foreign affairs agency.

OIG is addressing consolidation issues on a number of fronts. Prior to the legislation merging the foreign affairs agencies, OIG reviewed the consolidation of the security function in USIA and the Department. We determined that USIA's Office of Security could be merged with the Department's Bureau of Diplomatic Security resulting in more streamlined security activities. We identified about $500,000 in funds that could be put to better use, including up to 10 positions that could be used for other purposes in the security area. USIA's security staff will be formally integrated in October 1999 into the Department's Bureau of Diplomatic Security pursuant to the recent omnibus appropriations legislation.

The merger of the foreign affairs agencies also raises several challenges in the area of personnel management. Numerous policies and practices that differ between the Department and USIA such as assignment procedures, language training, tenuring regulations, and Senior Service competition rules will have to be reconciled. The Department has stated its intention to offer increased opportunities for retraining and upgrading employee skills and to work with USIA staff to integrate public diplomacy into the curriculum at the Foreign Service Institute.

Overseas tours of duty is another example where personnel policies differ between agencies. The Department's current policy of 2- and 3-year tours for staff at virtually all overseas posts (no 4-year tours) differs from other government agencies, including USIA, which currently has more than 50 4-year tours. A recent OIG review found that longer tours would reduce costs, and increase employee productivity. Costs could be reduced because longer tours would reduce the number of times employees move--the average cost of a move was over $18,000 in fiscal year 1996. Also, because of the considerable time necessary to become oriented to a new post, and the time at the end of the tour to bid for and transfer to the next post, longer tours would increase the time employees were fully productive in their current position.

Several studies by the Department and other groups have also recommended lengthening tours to improve effectiveness and achieve cost savings. However, in January 1999, Department officials announced that they would apply the Department's tour length policy when the foreign affairs agencies are consolidated, rather than adopt longer tours. In our view, this is a missed opportunity for the Department to increase the effectiveness of overseas personnel while also achieving cost savings.

The consolidation of foreign affairs agencies also presents a challenge to incorporate the best use of technology by USIA into the Department. The Department faces the challenge of effectively merging its decentralized information resources management organization with USIA's highly centralized system -- at a time when both

agencies are working to resolve Y2K problems in their respective systems. In addition, connecting USIA systems to Department systems must take into account necessary security considerations.

The pending merger of USIA and the Department has raised the issue of whether USIA's Y2K certification efforts meet the stringent standards set by the Department. USIA's current certification process is of concern because its guidelines do not contain the same level of detail and specificity used by the Department. When USIA merges with the Department in October 1999, USIA functions and the systems that support those functions will become the Department's responsibility. As such, we believe it would be prudent for the Department to assure itself that USIA's systems are evaluated for Y2K compliance on the same basis as Department systems.

Financial management challenges are also associated with the consolidation of foreign affairs agencies. This includes integrating USIA and ACDA into the Department's Central Financial Management System. The preparation of accurate and timely agencywide financial statements which include data from each agency will be necessary. Complicating the process is the fact that neither ACDA nor USIA is currently required to prepare audited financial statements under the Government Management Reform Act.

The consolidation of the Department and ACDA is mandated to occur on April 1, 1999; therefore, ACDA will be included in the Department's FY 1999 financial statements. Because ACDA is a fairly small agency in relationship to the Department, no significant problems are expected from the consolidation of the financial information. The consolidation of financial information with USIA is more significant and complicated. The Department and USIA will consolidate on October 1, 1999, which means the consolidated information would be reflected in the Department's FY 2000 financial statements. However, to facilitate the preparation of the consolidated statements, as well as provide a proper accounting of assets to be transferred to the Broadcasting Board of Governors, USIA should, at a minimum, prepare an audited balance sheet for FY 1999.

More Effective, Efficient, and Secure Operations and Infrastructures

The ability of the State Department, ACDA, and USIA to advance the foreign policy interests of the United States and their respective missions depends upon the quality of agency operations and infrastructure. Readiness to promote national interests and represent the United States to the world requires high-performance organizations with efficient and effective supporting systems.

As demonstrated by the terrorist attacks on U.S. embassies in Nairobi and Dar Es Salaam, perhaps no greater challenge exists for the Department than providing adequate

security to protect our people, facilities, and information. In response to the bombings, the Department is aggressively addressing physical security vulnerabilities and enhancing emergency planning at our overseas posts. I have also taken a number of steps to significantly enhance the security oversight operations of my office.

The foreign affairs agencies also face challenges in other areas related to operations and infrastructures. Generally, the Department is moving ahead on preparing computer systems for the Year 2000 date change, and expects to have 55 of its 59 mission-critical systems implemented by the OMB deadline of March 31, 1999. Despite this progress, we are concerned that the Department's Y2K certification process is proceeding too slowly.

In the area of financial management, the Department's financial and accounting systems are inadequate, and there are significant concerns with the security of financial systems on the Department's mainframe computer systems. In property management, the Department has yet to establish a baseline of maintenance and repair requirements and costs for overseas property.

Addressing Security Vulnerabilities

The bombings of U.S. embassies in Nairobi and Dar Es Salaam underscored the vulnerability of some of our posts and changed the approach to security at our missions for both the Department and OIG. Prior to the bombings in Africa, the Department generally allocated security resources to overseas posts based on the threat category of the city in which the diplomatic facility was located. The Department used threat information from a variety of intelligence and other sources and published a classified "Composite Threat List." Threats fell into four categories: political violence, human intelligence, technical intelligence, and crime. Threat levels in each of these categories ranged from critical to low. Embassies with a "critical threat" rating were generally allocated more funds for security enhancements than those embassies with "low threat" ratings. The bombings of our embassies, however, have caused the Department and intelligence community to recognize that the threat has changed dramatically and the allocation of resources based primarily on the use of the Composite Threat List is inadequate. In addition to the threat rating, the Department now factors in the vulnerability of all posts to terrorist attacks. Under this new approach, all posts should meet a high level of protection against acts of terrorism and political violence.

In response to the attacks on our embassies last year, the Department conducted an extensive review of mission security around the world and identified eight facilities so vulnerable that the missions will be moved into safer, more secure facilities as quickly as possible. In Nairobi, the mission is moving into interim office buildings that will provide a degree of security until new office buildings can be constructed and occupied. In Dar Es Salaam, such a move has already taken place. Construction of new embassies in these countries is scheduled to be complete by 2003. The Department also plans to undertake significant renovations to address serious vulnerabilities at other locations.

To enhance emergency response, the Department plans to spend $118 million on its wireless communications program. This will serve to upgrade the entire emergency radio program and send new radios to every overseas post for use during an emergency. The Department is also planning to purchase satellite telephones so that posts and emergency response teams can depend on reliable communication during and after an emergency.

Staffing shortages in security have been addressed by the recent supplemental appropriation, and the Department is engaged in an aggressive recruitment program for both security officers and security engineers to increase its workforce. However, the training period in the Department before new security officers gain the expertise to perform successfully overseas has historically taken up to 6 years. The new officers will be going overseas with only 2 or 3 years of experience. To examine the adequacy of the Department's support of these new officers, we plan to review the Bureau of Diplomatic Security's overseas operations management in the coming year.

I have taken a number of steps to significantly enhance the security oversight operations of my office. First, we have expanded our security oversight inspections to include low and medium threat posts. Also, routine post management inspections now include an experienced security officer who focuses on physical security and emergency preparedness, and prepares a classified security annex to the inspection report. This year we plan to complete 31 security oversight inspections. We also will complete security audits of the card access control program, protective details, the protection of classified information, and overseas telephone security.

Second, our new Security Enhancements Oversight Division will provide oversight of the $1.4 billion in emergency security funds, and future funding received by the Department, to enhance overseas security. OIG will evaluate physical and technical security being built into the new office buildings in Nairobi and Dar Es Salaam. In addition, OIG will examine security for construction personnel, on-site construction, logistics for items used in the controlled access areas, and contract management at these posts. This Spring, an inspection team will evaluate the security at the interim office building in Dar Es Salaam and the temporary office building in Nairobi.

Because a large portion of the emergency supplemental funds will go toward procuring goods and services and the construction of new facilities, OIG plans to provide audit assistance to ensure that contract costs are reasonable. OIG may audit selected contractors prior to award and at contract completion, and provide technical support to Department contracting officers in reviewing contractor proposed costs.

OIG already provides oversight of the embassy construction project in Moscow, Russia. The Moscow Oversight Team, established in 1994, provides oversight to the Moscow chancery construction project. The team was formed in response to the costly security mistakes that characterized previous construction efforts of Embassy Moscow. Rather than waiting to identify problems after the construction is complete, we have undertaken this ongoing oversight effort in order to flag potential vulnerabilities so that

they can be addressed promptly. With this approach we are contributing our expertise to facilitate project completion on time, within budget, and in a secure manner.

Another important oversight project for OIG will be the China 2000 initiative, which is scheduled to enter the design phase in FY 1999. The Department will have to respond to several formidable challenges in order to construct secure compounds. Construction security oversight is critical to ensuring that the China 2000 project adequately addresses security needs, and that security systems, once designed, will function as intended.

For several years, my office has reported that the Department faced significant challenges in managing and funding security and made numerous recommendations to address specific vulnerabilities at our missions worldwide. The Department has generally corrected deficiencies identified by OIG where they have had resources available to do so. Of the 588 security recommendations made in FY 1997, the Department agreed to correct approximately 90 percent of the deficiencies and completed action on about 50 percent within one year after they were identified.

However, many of the recommendations still outstanding are significant, and require major capital investments to implement. Examples include relocating missions to safer facilities, building safe havens, or improving walls that surround the facility. To meet these challenges, the Under Secretary of Management formed a number of coordinating groups in which she has welcomed full OIG participation. Despite the recent emergency appropriation, the Department continues to face funding shortfalls. Security equipment will also need long-term funding. A 1998 OIG audit of the maintenance and repair of security equipment found that, despite the fact that much of the Department's equipment, purchased in the mid-1980's, was reaching the end of its useful life or was obsolete, the Department's budget, as submitted to Congress, did not include funding for new equipment.

OIG's ongoing audit of overseas card access systems has found similar problems with equipment maintenance in the posts that we have reviewed. The Department lacked a uniform program for the installation, repair, and maintenance of the card access system equipment. In addition, the equipment was never certified for use and, in some cases, was locally procured and maintained. Furthermore, we have serious reservations as to whether the card access control systems can effectively control access and protect sensitive information without the integration of other security measures. Our security inspections have repeatedly demonstrated that security at "lock-and-leave" posts without 24-hour cleared U.S. Marine Guard protection is often inadequate to protect classified material.

Emergency Preparedness

As a result of our audit on emergency evacuation, the Department reinstated its crisis management exercise program, which trains emergency action committees at posts on how to manage crises more effectively. The ability of posts to respond to emergencies, such as natural disasters or terrorist attacks, is greatly enhanced by the

Department's crisis management exercises and emergency drills. However, our security inspections consistently report that posts are not conducting the required drills needed to prepare for likely attacks. In addition, we recently reported to the Bureau of Diplomatic Security on specific steps it should take to enhance procedures for vehicle bomb drills. The Accountability Review Board strongly recommended the immediate institution of "duck and cover" drills. Our security inspection teams recommended regular practice of these drills along with specific recommendations for immediately alerting staff to vehicle bomb attacks. Our Chiefs of Mission have quickly embraced these recommendations, but our most recent security inspections found that neither the Department nor posts have identified how to best implement the drills and warning procedures.

Strengthening Information Security

The Department faces significant challenges in information systems security. Our work has pointed out deficiencies in the Department's mainframe and communication systems security, including incomplete and unreliable security administration, inadequate training, and lack of access control. Similar problems have been identified in the specialized computers used in telephone switching and in card access systems. The Department has provided security coordination and guidance to assist in the development of some critical computer systems and software. However, in other cases, particularly telecommunications, the Department is modernizing systems without a parallel effort to improve information security. A May 1998 General Accounting Office audit report reiterated our findings on the need for improved management of information security.

We remain concerned about the Department's backup capability for its major information systems. OIG has addressed this vulnerability in 3 audit reports since 1988, when Congress provided funding for the backup facility now located in Beltsville, Maryland. In 1998, the Department confirmed that it should now have the physical capacity to address a loss of unclassified mainframe systems at the Department or in Beltsville. The OIG expects to review the Department's progress in meeting our earlier concerns to ensure those backup sites and systems currently in place are effective. We will also assess whether issues involving planning, coordination, training and resources are resolved and whether contingency plans are fully tested.

The Department has told the OIG that it has established a security program for the mainframe system to address risks earlier identified by OIG and to ensure that responsible officials are identified and kept informed about the systems security. We will continue to monitor the Department's efforts. We have also recommended that the Department require personnel who hold positions with access to bulk quantities of sensitive information to undergo a special counterintelligence screening process prior to each assignment. This last issue will be addressed in an OIG audit of counterintelligence programs scheduled to begin in April 1999.

Achieving Y2K Compliance

Another critical challenge facing the foreign affairs agencies is their vulnerability to the Y2K problem. Generally, the Department is making steady progress toward

ensuring that it is ready for the Year 2000 date change. As of March 1, 1999, the Department reported that 39 of 59 mission-critical systems are compliant and fully implemented, and it expects to have 55 mission-critical systems implemented by the March 31, 1999, OMB deadline. Despite this progress, we are concerned that the Department's Y2K certification process, which is designed to provide documented independent assurance that all possible steps have been taken to prevent Y2K-related failures, is proceeding too slowly. Thus far, only two mission-critical systems have been certified by the Department's Y2K Certification Panel.

Year 2000 compliance and adequate contingency plans are necessary to avoid creating havoc in the foreign affairs community, including disruption of messaging systems, impediments to embassy operations such as visa and passport processing, and failures in administrative functions such as payroll and personnel processing in the Year 2000. The Department's presence at more than 260 locations worldwide increases the Department's challenge to continue functioning effectively in the Year 2000. Embassies and consulates rely on their respective host countries' infrastructures to provide essential, day-to-day services such as power, water, telecommunications, and emergency services. In some countries these services could be disrupted if critical infrastructure components and control systems are not made Y2K compliant.

My office has been actively engaged in Y2K efforts in three major areas. First, we assisted the Department in its efforts to develop certification guidelines identifying what steps the Department must take to determine whether systems are Y2K compliant, and identified documentation needed to certify computer systems as "Year 2000 ready." OIG is also evaluating the adequacy of certification packages prepared by bureaus for mission-critical systems. Second, we are reviewing Department and USIA efforts overseas to prepare adequately for the millennium change. This effort includes monitoring activities of our overseas posts to raise global awareness of the Year 2000 problem, ensuring that U.S. embassy and consulate system vulnerabilities are properly addressed, and reviewing post contingency plans. Finally, because U.S. embassies and Americans living and working abroad might be vulnerable to Y2K-related infrastructure failures, we are assessing the Y2K readiness of host countries where the U.S. Government maintains a presence.

Our work with the Department has resulted in several improvements. OIG findings resulted in greater focus on Departmentwide project management tracking; discovery of seven new applications, which were added to the Department's system-tracking database; and development of a new rating system that tracks and evaluates system interfaces.

OIG has conducted site assessments in 25 cities in 20 countries as part of an aggressive effort to review embassy preparedness and collect and analyze information on host country Y2K efforts. Early on, OIG found little contingency planning at posts in the event of a failure of basic infrastructure services on January 1, 2000. The Department is aware of this problem, and has sent a Contingency Planning Toolkit to all embassies and consulates to assist them in developing their respective plans.

In our effort to assess the readiness of host countries to address Y2K-related problems, OIG has met with representatives from foreign governments, key infrastructure sectors, and private industry in each country we visited. We have provided information summaries on each of these countries to the Department, USIA, the President's Council on the Year 2000 Conversion, congressional committees, and other foreign affairs organizations.

OIG has initiated a series of USIA Worldnet Interactive broadcasts throughout Latin America and Canada. In coordination with the Organization of American States and USIA, these interactive programs have been broadcast live throughout this hemisphere and worldwide via the internet to explore problems, strategies and solutions in the areas of timely contingency planning, energy and financial institutions readiness, and auditing techniques to promote Y2K compliance.

Correcting Weaknesses in Financial Management

Financial management continues to be another major challenge facing the foreign affairs agencies. The Department accounts for more than $5 billion in annual appropriations and over $16.7 billion in assets. The Department has made significant improvements in financial management since the Chief Financial Officer's Act was passed in 1990. OIG has focused on the Department's financial management through our audits and annual review of the Department's progress to improve material weaknesses in conjunction with the preparation of the Federal Manager's Financial Integrity Act (FMFIA) report. Over the past few years, the Department has complied with OIG recommendations in areas such as disbursing, cashiering, travel advances, and accounts receivable, which significantly improved these areas and led to these weaknesses being removed from the FMFIA report.

However, a number of significant concerns still exist, some of which have been outstanding for a number of years. Although OIG's audit of the Department's 1997 agencywide financial statements resulted in a clean opinion, the report brought to management's attention significant concerns with the security of the Department's domestic main frame computer.

OIG's audit of the Department's 1997 agencywide financial statements also raised concerns about the inadequacy of the Department's financial and accounting systems, which is both an internal control weakness and an issue of noncompliance with several laws and regulations, including the Federal Financial Management Improvement Act (FFMIA). The FFMIA requires that agencies report whether the Department's financial management systems substantially comply with the Federal financial management system requirements and applicable accounting standards. Based on our review, OIG found that the Department does not substantially comply with one aspect of the FFMIA, that is the Federal financial management system requirements. The Department has reported its financial systems as a material nonconformance since 1983 in its annual FMFIA report.

OIG has urged the Department to focus attention on its financial systems and to develop benchmark performance indicators to measure the improvements to these

systems. In response to our recommendations, the Department is planning to study the level of compliance with the FFMIA and to prepare a remediation plan as required by that Act. The Department has also upgraded the Central Financial Management System, and has other improvement efforts underway, such as developing a replacement for the existing overseas regional systems.

Issues regarding timeliness of the financial statements and data, internal controls over major processes, and presentation of data for new requirements have yet to be resolved. OIG's last two audits of the financial statements identified issues related to unliquidated obligations. Although we have recommended that the Department focus on this area, our preliminary audit work on the Department's 1998 financial statements shows that these weaknesses persist.

In addition, we have recommended that the Department ensure that adequate resources are devoted to financial statement preparation, especially for the FY 1998 financial statements due to the increased reporting requirements. Based on our preliminary work, however, we have found that the Department is still unable to provide certain financial documentation by the agreed upon deadlines.

Grants management is another area of financial management weakness in USIA, and needs to be carefully considered in the consolidation with the Department. USIA annually awards about 500 domestic grants and cooperative agreements totaling approximately $240 million, about 1500 overseas grants totaling about $20 million, and numerous transfers to bilateral commissions and foundations totaling $120 million. OIG's audits have identified unauthorized, unallowable, and unsupported costs, internal control weaknesses, or noncompliance with applicable regulations associated with these awards. For example, OIG identified about $1 million in surplus funds at the Fulbright commission in India. USIA fully implemented our recommendation to offset the commission's 1998 allocation resulting in a one-time cost savings. Screening and monitoring of the recipients of these funds will become more critical because under revised Office of Management and Budget guidelines, the majority of USIA's grantees will no longer be required to have annual financial audits.

Overall, Federal assistance in the form of grants, cooperative agreements, transfers, or loans from the Department, USIA, and ACDA total over $1 billion annually. For example, the Department's migration and refugee assistance programs alone amounted to $650 million in FY 1998. The Department is currently considering alternatives to managing grant activities once consolidation occurs.

Improving Real Property Management and Maintenance

Currently the Department reports holding 12,000 properties with an estimated historical cost of about $4 billion. OIG has identified problems in the Department's procedures for the disposition of real property. These findings contributed to language in the Conference Report accompanying the FY 1997 Omnibus Appropriations Act requiring the establishment of a Real Property Advisory Board to help reduce the Department's inventory of surplus real property overseas. OIG has completed a review of

the activities of the Board, and found that disputed properties are appropriately chosen for the Board's review and recommendations of the Board are based on sufficient information.

At the request of the Under Secretary for Management, OIG is working with the Department to assist in identifying excess, underutilized, and obsolete government-owned and long-term leased real properties worldwide. OIG has conducted limited reviews of real property in the course of its ongoing audits and inspections at overseas posts. Since March 1998, OIG has provided the Department with 29 final reviews on 37 overseas sites, 6 draft reviews on 11 overseas sites, and is in the process of completing reviews on another 24 overseas sites. The reviews can be used by the Department to manage the acquisition and disposition of overseas real property assets.

To date, OIG reviews have identified 5 properties as excess and 81 properties underutilized. An example of an underutilized property includes a nearly 1-acre unpaved site near the chancery building in Paris used to provide parking for official vehicles and some embassy employees. According to post officials, there were plans to construct an office building on the site in the mid-1980's, but those plans had been rejected. The Department has no plans to develop this site, and has stated that the site is serving an essential purpose as a secure vehicle parking area. Recently the post has reported that the property is needed for security and operational concerns. OIG will review these concerns during its April-May 1999 security oversight inspection of Embassy Paris.

OIG reviews also identified 6 properties as obsolete. For example, OIG has identified two obsolete properties at Embassy Harare, and has recommended the Department give them immediate attention for disposal action. Additionally, OIG reviews noted 35 properties that the Department had previously identified for future development or disposal when local economic conditions become favorable. Examples include properties in Bangkok, Seoul, and Kathmandu.

The Department and overseas posts have recently addressed many real property maintenance and repair issues, in part, due to the work of the OIG. In 1993, OIG recommended that the Department establish a system to identify and monitor the worldwide maintenance and repair requirements and establish an initial baseline for outstanding maintenance and repair requirements. In response to the recommendation, the Department has established a system to identify and monitor requirements, but has not analyzed the information contained in that system to establish a baseline of maintenance and repair requirements and costs. Future OIG work will evaluate the Department's systems of identifying, prioritizing, and performing maintenance and repair.

*** * ***

In conclusion, Mr. Chairman, I have outlined the major management challenges facing the foreign affairs agencies we oversee. The Department has made notable improvements in longstanding areas of concern to OIG, including border security, financial management, and the establishment of a Chief Information Officer. Overcoming other challenges will require careful and long-term management attention.

However, in some significant areas, the Department will not be able to address these problems without the assistance of Congress. As I have testified today, the most significant, immediate need is to ensure the safety and protection of U.S. Government assets overseas. The Department needs the long-term commitment of Congress to address these critical security vulnerabilities.

I look forward to working with members of this subcommittee in the coming year on many of these issues. I would be pleased to answer any questions you may have.